Course Description

McAfee Network Data Loss Prevention Administration

Intel Security Education Services Administration Course

The McAfee® Data Loss Prevention Administration course enables attendees to receive in-depth training on the benefits of the centralized management and deployment of McAfee network data loss prevention products including DLP Manager, Prevent, Discover, and Monitor. Enabling administrators to fully understand the capabilities of their security solution not only reduces the risks of misconfiguration, but also ensures that an organization gets the maximum protection from installation and usage. At the end of this course, attendees should understand the capabilities of McAfee NDLP products and have the ability to install and configure McAfee NDLP Manager, Prevent, Discover, and Monitor in a production environment. Students will also learn how to customize policy, generate reports and optimize their data loss prevention environment.

Course Goals

- Installation and administration of McAfee Network Data Loss Prevention appliances
- Case-based policy configuration and deployment
- Incident management and case workflow
- Policy tuning and best practices
- Reporting

Agenda At A Glance

Day 1

- About the Course
- DLP Overview
- NDLP Product Offerings
- DLP Common Elements
- Case Studies
- DLP Installation
- DLP Manager
- DLP Users and Groups

Audience

- System and network administrators, security personnel, auditors, and/or consultants concerned with network and system security should take this course.

Register Now for Training

intel Security

Agenda At A Glance Continued

Day 2

- DLP Policies
- DLP Rules
- Rule Content
- Rule Context
- Other DLP Rule Elements
- Action Rules
- **DLP Monitor**
- **Monitor Policy**

Day 3

- DLP Discover
- Discover Policy
- Email Prevent
- Email Prevent Policy
- Web Prevent
- Web Prevent Policy

Day 4

- Incident Management
- Dashboard and Reporting
- Rule Tuning and Best Practices
- Case Study Review

Recommended Pre-Work

It is recommended that the students have a working knowledge of Microsoft Windows administration, system Administration concepts, a basic understanding of computer security concepts, and a general understanding of viruses and anti-virus technologies.

Course Outline

Module 1: About the Course

- Course Overview
- Facilities
- Introductions
- McAfee Education Services
- McAfee Product Training
- Foundstone Security Education
- McAfee Technical Support
- McAfee Security Content Release Notes
- Product Enhancement Request
- McAfee Community
- Helpful Links
- Classroom Lab Setup
- Using the Lab Guide
- Resources
- Acronyms and Terms
- NDLP Documentation
- Helpful Links to Bookmark

Module 2: DLP Overview

- The Borderless Business Environment
- Data Breaches in the Headlines
- Data Breaches Don't Discriminate
- Data Concerns
- The costs involved in data loss
- Key DLP solution requirements
- Data Loss Vectors
- "We all contribute to it."
- The McAfee Approach
- Data Concerns
- The costs involved in data loss
- Product Documentation Source

Module 3: NDLP Product Offerings

- DLP Solution Offering
- McAfee DLP Products
- NDLP Ports
- Supported Systems
- Compatible McAfee products
- Supported repositories
- Supported browsers

Course Description

- Supported languages
- NDLP Manager
- NDLP Monitor
- Capturing Data
- Mirror Port and Network Tap
- NDLP Discover
- DLP Discover
- NDLP Prevent
- NDLP Prevent (Email)
- NDLP Prevent (Web)
- Deployment Checklist
- Connectivity requirements and limitations
- Implementation Process Checklist
- Change Control

Module 4: DLP Common Elements

- Policy and Rule Checking
- Policies
- Policy Configuration
- NDLP Capture Database
- Case Management
- NDLP Case Workflow
- Dashboard and Reporting
- Dashboard
- Search list – Results
- Lab Exercises

Module 5: Case Studies

- Deployment Scenarios
- Main DLP Drivers for Health Care
- Health Care Use Case
- Health Care Information to Protect
- Main DLP Drivers for Manufacturing
- Chemical Manufacturer Case
- Chemical Information to Protect
- Main DLP Drivers for Banking
- Data Breaches - Larger Organizations
- Banking Case
- Banking Information to Protect

Module 6: DLP Installation

- DLP Hardware
- NDLP Physical Appliances
- DLP Hardware
- NDLP Server Ethernet ports
- VMware
- NDLP Images
- NDLP Boot Menu - 4400/5500/ Virtual
- Software Install/Upgrade (utilities for install)
- Software Install/Upgrade (utilities for install)
- Steps to install DLP Software
- Switching on the appliance for the first time
- NDLP Manager Initial Configuration
- NDLP Manager Initial Configuration
- NDLP Configuration
- Installation Troubleshooting
- Implementation Process Checklist
- Change Control

Module 7: DLP Manager

- What is NDLP Manager?
- NDLP Manager Key Features
- NDLP Manager Best Practices
- Firewall Configuration (Port Information)
- Firewall Configuration (Port Information)
- NDLP Manager UI – HOME
- NDLP Manager UI – INCIDENTS
- NDLP Manager UI – CASE
- NDLP Manager UI – SEARCH
- NDLP Manager UI – POLICIES

Course Description

- NDLP Manager UI – CLASSIFY
- NDLP Manager UI – SYSTEM
- NDLP Manager UI – Adding a new Device
- NDLP Disaster Recovery Features
- Lab Exercises

Module 8: DLP Users and Groups

- DLP Users and Groups
- Managing Users and Groups
- Failover account
- Users
- Adding a New Local User
- Groups
- Groups and Business Units
- NDLP Group Properties
- Task Permissions
- Policy Permissions
- NDLP LDAP User
- Create a Directory Server
- Adding a LDAP User
- Logging in with LDAP user
- Troubleshooting Directory Server Issues
- Troubleshooting Directory Server Issues
- McAfee Login Collector (MLC)
- Creating McAfee Login Collector
- Lab Exercises

Module 9: DLP Policies

- NDLP Policy
- Policy Configuration
- Policy Definition
- Regional Policy Selection
- Policy Actions
- Activating and Deactivating a Policy
- Creating a Policy - Add Policy Screen
- Creating a Policy - Edit Policy Screen
- Policy Ownership
- Policies and Rules
- Searching
- Policy Advanced Settings
- Lab Exercises

Module 10: DLP Rules

- Rule Checking
- Rule Definitions
- Rule Tabs
- Adding (Creating) a Rule From a Search
- Rule Creation
- Rule Management
- Define
- Action
- Exceptions
- Restricting Data Matches

Module 11: Rule Content

- Rule Content
- Templates
- Keyword
- Keywords and Stems
- Content Type
- Combining multiple definitions
- Using Templates
- Expressions
- Commonly Used Expressions
- In NDLP concepts, what are \k and \K used for?
- Expression Examples
- Using Expressions
- Concept
- Concepts
- Adding a Concept
- Concept Algorithms
- Managing Concepts

Course Description

- Duplicating Concepts

Module 12: Rule Context

- Context
- Adding Context to a Concept
- Count
- Percentage Match
- Location
- Proximity – distance
- Proximity
- Proximity Order
- Concept Example
- Context Examples
- Lab Exercise

Module 13: Other DLP Rule Elements

- Other Rule Elements
- Source/Destination
- Email Addresses
- IP Address
- URL match
- GeoIP Location
- File Information
- Document Properties
- Adding a Document Property
- Protocol/Port
- Discover
- Date/Time
- Lab Exercises

Module 14: Action Rules

- Action Rules
- Adding a new Action Rule
- E-mail Options
- Syslog
- Incident Reviewer
- Incident Status
- Action Rules
- NDLP Rule Actions
- Lab Exercises

Module 15: DLP Monitor

- What is NDLP Monitor?
- NDLP Monitor
- Using multiple monitors
- Monitor Architecture
- Mirror Port / Network TAP
- Capture Filters
- Network and Content Filters
- Network Filter Action Types
- Sample Network Capture filter
- RFC 1918
- Content Filter Action Types
- Sample Content Capture filter
- Searching from the GUI
- Search Tasks Permissions
- Basic search – example
- Advanced search – Example
- Search list – Details
- Search list – Results
- Search tasks
- NDLP Appliance Installation
- Quick Start Wizard
- Registering NLDP appliances
- NDLP Appliance Registration
- Lab Exercises

Module 16: Monitor Policy

- Data-in-Motion Policy
- Data-in-Motion Action Rules
- Data-in-Motion Policy
- DiM Search Results
- Checking the RFS Disk Space
- Disk Usage
- Troubleshooting – Data not being captured
- Troubleshooting – Check Port

Course Description

Configuration
- Troubleshooting – Network
- Troubleshooting – Check Filters
- Troubleshooting – Summary
- Lab Exercises

Module 17: DLP Discover
- Scans
- DLP Discover
- Supported Repositories
- Supported Databases
- DLP Discover Architecture
- Scan Types
- Four types
- Concurrent Scan Tasks and Crawl Rate
- Inventory Scans
- Firewall Configuration (Port Information)
- Classification Scans
- Registration Scans
- Data Registration
- About Signatures
- Description of Signature Types
- Discover Scans
- Discover Scan Remediation
- Before Setting Up a Scan
- Adding Discover to DLP Manager
- Lab Exercises

Module 18: Discover Policy
- NDLP Discover Scans
- Schedules
- Credentials
- Export Locations
- SSL Enabled Database Crawling
- Scan Actions
- Scan States
- Scenario – Creating scanning for PII
- Inventory Scan
- Node Definition
- Checking Credential for a Single IP
- Node Definition Filtering
- Filters
- Advanced Options
- Advanced Options – Rate Control
- Running a Scan
- Scan Results
- Classification Scan
- Data Classification
- Classification Scan – Data Classification
- Predefined View – OLAP Navigator
- Discover Scan
- Discover Scan Policies
- Discover Scan Remediation
- Action Rule Remediation
- Incident Remediation
- Registration Scan
- Lab Exercises

Module 19: Email Prevent
- What is NDLP Email Prevent?
- Architecture: Prevent-Email
- NDLP Prevent Redundancy
- Deployment Guidelines – Prevent Email
- Firewall Configuration (Port Information)
- Prevent Network/Content Filters
- Steps to Integrate MEG with DLP Prevent
- MEG Policy – Direct to NDLP Prevent
- MEG Policy – Custom Header Dictionary
- MEG Policy – Post NDLP Prevent

Policy
- MEG Compliance Rules
- NDLP Prevent MTA Access
- Lab Exercises

Module 20: Email Prevent Policy
- NDLP Email Prevent
- NDLP Email Prevent Actions
- Allowed Actions for NDLP Email Prevent
- NDLP Email Prevent Policy Flow
- NDLP Policy Configuration
- NDLP Action by Appliance
- NDLP Prevent Policy
- NDLP Prevent Troubleshooting
- Tcpdump
- Mailq
- Maillog
- Lab Exercises

Module 21: Web Prevent
- What is NDLP Web Prevent?
- Data Flow
- NDLP Prevent Redundancy
- Deployment Guidelines – Prevent Web
- Firewall Configuration (Port Information)
- Steps to Integrate MWG with DLP Prevent
- Add Library Rule
- Rule Set Position
- Data Loss Prevention with ICAP Rules
- ReqMod Setting

Module 22: Web Prevent Policy
- NDLP Prevent (Web) Policy
- NDLP Prevent (Web) Block Page
- NDLP Prevent (Web) Policy
- www.csm-testcenter.org
- NDLP Prevent Troubleshooting
- Tcpdump
- Lab Exercises

Module 23: Incident Management
- Case Management
- DLP Incident Management
- Supported Incident Types
- Incident Management-Managed Appliances
- Incident Management on the Manager
- Incident Dashboard – Incident Types
- Incident Viewing Formats
- Viewing Incidents in Different Formats
- Viewing Incidents in Different Formats
- Incident Actions
- Incident Dashboard Options
- Incident Views and Scheduled Reports
- Policy Permissions for Incidents
- Incident Remediation Workflow
- Case and Incident Management
- Creating a Case
- Creating a Case from Incidents
- Adding Incidents to an Existing Case
- Customize Case Config Option
- Customize Case Config Page
- Case Attachment
- Case Management Permissions
- Case Level Permissions
- Group Task Permissions for Cases
- Case Permissions - Summary
- NDLP Case Workflow
- Case Management Best Practices

Course Description

- Case Management Workflow Example
- Lab Exercises

Module 24: Dashboard and Reporting

- Dashboard and Reporting
- Pre-defined Table and Charts
- Risk Analysis Chart
- Customizing Homepage & Charts
- Network Statistics
- Exportable Incidents
- Exportable Cases
- Exportable Searches
- Customizing Export Data
- Lab Exercises

Module 25: Rule Tuning and Best Practices

- False Positives
- Reducing False Positives
- Network Filters
- Content Filters
- Policy – Suppress Incidents
- Rule Modification
- Rule Tuning
- Rule Tuning – Proximity
- Rule Best Practices

Module 26: Case Study Review

- Deployment Scenario Review
- McAfee Medical Services
- Health Care – Consolidate Files
- Health Care – Restrict File Transmission
- McAfee Chemical Corporation
- Chemical Company – Notify IP detection
- Chemical Company – Allow PI transmission
- McAfee Federal
- Banking - Rule Sensitivity
- Banking – Incident/Case Management

To order, or for further information, please contact McAfee Education at: 1-866-210-2715.

NA, LTAM, and APAC: education@mcafee.com

EMEA: proserv@mcafee.com